日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

#3

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed in this Office.

出 願 年 月 日
Date of Application: ２０００年 ６月２０日

出 願 番 号
Application Number: 特願２０００－１８４７７８

出 願 人
Applicant (s): カシオ計算機株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２００１年 ３月 ９日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０１７２６８

【書類名】　特許願
【整理番号】　00-0089-00
【提出日】　平成12年 6月20日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
【発明者】
【住所又は居所】　東京都羽村市栄町３丁目２番１号　カシオ計算機株式会社羽村技術センター内
【氏名】　竹田　恒治
【特許出願人】
【識別番号】　000001443
【氏名又は名称】　カシオ計算機株式会社
【代理人】
【識別番号】　100093632
【弁理士】
【氏名又は名称】　阪本　紀康
【電話番号】　03-3238-0058
【手数料の表示】
【予納台帳番号】　012900
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9004585
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ暗号化装置及びデータ復号化装置

【特許請求の範囲】

【請求項１】平文データの物理的あるいは論理的構造をブロック化するブロック化手段と、

該各ブロックについて、暗号処理を行う際に使用する暗号化属性を設定する暗号化属性設定手段と、

該暗号属性に基づいて、各ブロックを暗号化することによって、暗号文データを生成する暗号化手段と、

該暗号文データと該暗号属性とを暗号結果として出力する出力手段と、

を備えることを特徴とするデータ暗号化装置。

【請求項２】前記暗号化属性と前記暗号文データを別ファイルとして格納することを特徴とする請求項１に記載のデータ暗号化装置。

【請求項３】前記暗号化属性と前記暗号文データとを１ファイルとして格納することを特徴とする請求項１に記載のデータ暗号化装置。

【請求項４】前記暗号化属性は、ブロック化された平文データの各ブロックの位置を示す情報と、ブロックの大きさを示す情報と、該ブロックの情報にアクセスする権利を有するユーザを設定する情報と、暗号鍵に関する情報とを備えることを特徴とする請求項１に記載のデータ暗号化装置。

【請求項５】前記ブロック化手段は、前記ブロックを更に小さなサブブロックに分割し、

前記暗号化属性設定手段は、該サブブロックそれぞれについて暗号化属性を設定し、

前記暗号化手段は、該サブブロック単位での暗号化を行うことを特徴とする請求項１に記載のデータ暗号化装置。

【請求項６】前記暗号化手段は、前記サブブロック単位での暗号化はするが、前記ブロック単位での暗号化は行わないことを特徴とする請求項５に記載のデータ暗号化装置。

【請求項７】前記ブロックの暗号化を行った後、サブブロック化して、該サ

ブブロックを暗号化することを特徴とする請求項５に記載のデータ暗号化装置。

【請求項８】平文データをブロック化し、各ブロック毎に設定される暗号化属性に基づいて各ブロックを暗号化することによって暗号化された暗号文データを復号する復号装置であって、

該暗号文データと該暗号化属性を読み込む読み込み手段と、

該暗号文データを該平文データのブロックに対応するブロックに分割し、該暗号化属性に基づいて該ブロックを復号することにより、暗号文データを復号する復号化手段と、

を備えることを特徴とするデータ復号化装置。

【請求項９】平文データの物理的あるいは論理的構造をブロック化するブロック化ステップと、

該各ブロックについて、暗号処理を行う際に使用する暗号化属性を設定する暗号化属性設定ステップと、

該暗号属性に基づいて、各ブロックを暗号化することによって、暗号文データを生成する暗号化ステップと、

該暗号文データと該暗号属性とを暗号結果として出力する出力ステップと、

を備えることを特徴とするデータ暗号化方法。

【請求項１０】平文データをブロック化し、各ブロック毎に設定される暗号化属性に基づいて各ブロックを暗号化することによって暗号化された暗号文データを復号する復号方法であって、

該暗号文データと該暗号化属性を読み込む読み込みステップと、

該暗号文データを該平文データのブロックに対応するブロックに分割し、該暗号化属性に基づいて該ブロックを復号することにより、暗号文データを復号する復号化ステップと、

を備えることを特徴とするデータ復号化方法。

【請求項１１】平文データの物理的あるいは論理的構造をブロック化するブロック化ステップと、

該各ブロックについて、暗号処理を行う際に使用する暗号化属性を設定する暗号化属性設定ステップと、

該暗号属性に基づいて、各ブロックを暗号化することによって、暗号文データを生成する暗号化ステップと、

該暗号文データと該暗号属性とを暗号結果として出力する出力ステップと、

を備えることを特徴とするデータ暗号化方法を情報装置に実現させるプログラムを格納した、情報装置読み取り可能な記録媒体。

【請求項１２】平文データをブロック化し、各ブロック毎に設定される暗号化属性に基づいて各ブロックを暗号化することによって暗号化された暗号文データを復号する復号方法を情報装置に実現させるプログラムを格納した記録媒体であって、

該暗号文データと該暗号化属性を読み込む読み込みステップと、

該暗号文データを該平文データのブロックに対応するブロックに分割し、該暗号化属性に基づいて該ブロックを復号することにより、暗号文データを復号する復号化ステップと、

を備えることを特徴とするデータ復号化方法を情報装置に実現させるプログラムを格納した、情報装置読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、データ暗号化装置及びデータ復号化装置に関する。

【０００２】

【従来の技術】

今日、コンピュータの一般への普及やビジネスへの普及が著しく、従来手作業で行われていた手続がコンピュータによる処理によって取って代われて来つつある。このような状況の中、コンピュータによって扱われるデータの中には、個人のプライバシーに関わるなど、コンピュータネットワークなどを介してやりとりするにおいて、そのままのデータを使用するのでは、秘匿性が十分確保できないという状況が生じてきた。従って、そのようなデータを暗号化する必要があるのであるが、暗号化をコンピュータが行うの上で、十分安全かつ演算効率の良い暗号化方式が望まれている。

【０００３】

従来のデータ暗号化手法では、一般に、ストリームデータを幾つかの領域（ブロック）データに分け、各々のブロックに暗号化の処理を行い、データ全体としての暗号化を行っていた。その際、各暗号化ブロックに対するセキュリティレベルは同一に設定されていた。すなわち、各暗号化ブロックに使用される暗号が同じであり、かつ、同じアルゴリズムを使って各暗号化ブロックを暗号化していた。

【０００４】

【発明が解決しようとする課題】

上述したとおり、従来の暗号化手法では、一般に、ストリームデータを幾つかの領域（ブロック）に分け、各々のブロックに暗号化の処理を行い、データ全体としての暗号化を行っていた。その際、各暗号化ブロックに対するセキュリティレベルは同一に設定されていた。このため、暗号化されたデータの一部が解読されると、全てが解読されてしまうという危険性があるという問題点があった。

【０００５】

本発明の課題は、データの一部が解読されても全データは容易には解読されない暗号手法を用いた暗号化装置を提供することである。

【０００６】

【課題を解決するための手段】

本発明のデータ暗号化装置は、平文データの物理的あるいは論理的構造をブロック化するブロック化手段と、該各ブロックについて、暗号処理を行う際に使用する暗号化属性を設定する暗号化属性設定手段と、該暗号属性に基づいて、各ブロックを暗号化することによって、暗号文データを生成する暗号化手段と、該暗号文データと該暗号属性とを暗号結果として出力する出力手段とを備えることを特徴とする。

【０００７】

本発明の復号化装置は、平文データをブロック化し、各ブロック毎に設定される暗号化属性に基づいて各ブロックを暗号化することによって暗号化された暗号文データを復号する復号装置であって、該暗号文データと該暗号化属性を読み込

む読み込み手段と、該暗号文データを該平文データのブロックに対応するブロックに分割し、該暗号化属性に基づいて該ブロックを復号することにより、暗号文データを復号する復号化手段とを備えることを特徴とする。

【０００８】

本発明によれば、平文データの部分部分で暗号化の属性を変更することが出来るので、たとえ平文データの一部が解読されても他の部分が解読されることはなく、より信頼性の高い暗号化手法を提供することが出来る。特に、暗号属性をユーザが適宜定めることにより、よりユーザのニーズにあった暗号化を行うことが出来る。

【０００９】

【発明の実施の形態】

図１、及び図２は、本発明の第１の実施形態の概念を説明する図である。

図１（ａ）は、平文（Ｍ）の二次元配列データを模式的に示したものである。この図においては、映像データが二次元平面上に表されている。また、二次元的広がりを持った配列データとしては、他に、データベースの内容を表形式で表現したものがある。本発明の第１の実施形態においては、このように、データの論理的広がりが平面あるいは立体など多次元的となっているデータ配列に対する暗号化の方法を示す。もちろん、論理的構造が１次元的であっても同様に、本実施形態を適用可能である。

【００１０】

図１（ｂ）は、平文を幾つかのブロックに分けたものである。ここに、各ブロックの形状は任意に設定でき、同一の形状にしてもよく、各々が異なる形状であっても良い。ＭｎとＭに付した番号ｎはブロックの番号である。前述したように、従来においては、図１（ａ）のような平文データの全体を１つの固まりとして考え、この１固まりのデータを所定の暗号処理が行い安い領域に分割して暗号化し、全体にわたって、同じ鍵を用いて同じ暗号化アルゴリズムを用いて暗号化していた。

【００１１】

これに対し、本発明の第１の実施形態においては、例えば、図１（ａ）の二次

元的配列を持ったデータを図１（ｂ）に示すように、複数のブロックに分割し、それぞれに固有の暗号鍵及び／あるいは暗号化アルゴリズムを適用して、全体のデータを暗号化する。

【００１２】

図２（ａ）は、平文のブロックＭｎの暗号化を規定する属性Ａｎの表を示す。ここでは、ＭｎとＡｎの一対一対応が明確になるように図示されているが、実際には、この対応付けが正確になされれば、明示的に対応付けされていなくても良い。すなわち、図２（ａ）においては、平文のブロックＭ１に対応する暗号化処理の属性はＡ１であり、同様に、Ｍ２～Ｍ４のそれぞれのブロックに対応した暗号化処理の属性はＡ２～Ａ４である。しかし、このように、属性の対応のさせ方は、図２（ａ）のような二次元配列データの配列位置を対応するようにする必要はなく、平文（Ｍ）の分割ブロックそれぞれにポインタを付属しておき、このポインタが暗号化処理の属性が格納されている位置を示すように構成しても良い。

【００１３】

図２（ｂ）は、平文のブロックＭｎを暗号化の属性Ａｎで暗号化して得られた暗号のブロックＣｎを示している。すなわち、図２（ｂ）においては、平文Ｍ１に暗号化属性Ａ１を用いて暗号化した暗号データがＣ１であり、以下同様に、平文Ｍ２～Ｍ４のそれぞれに暗号化属性Ａ２～Ａ４を用いて暗号化していたものが暗号データＣ２～Ｃ４である。

【００１４】

ここで、暗号化属性Ａ１～Ａ４は、例えば、暗号鍵であったり、暗号化するためのアルゴリズムである。

また、図１、２では、平文のブロックＭｎと暗号のブロックＣｎとは同じ形状で表されているが、一般にはこれらの形状は異なっても良い。

【００１５】

上記のような暗号化方法によれば、暗号の二次元配列データ｛Ｃｎ｝と属性｛Ａｎ｝が保存されるため、平文の二次元配列データを得るには保存されている暗号の二次元データ｛Ｃｎ｝に対し｛Ａｎ｝で規定される暗号の属性を基に復号化の操作を行えばよい。

【００１６】

第１の実施形態では、平文の二次元配列データを幾つかのブロックに分け、その各ブロックの暗号化に属性を設けて暗号化したことにより、ブロック毎の暗号化時に暗号の属性をきめ細かく設定できるという効果がある。例えば、「このブロックは暗号化しない」という属性も付与することができ、暗号化データの安全性を損なうこと無く、暗号化データを全文検索の対象にし得るという実用上便利な性格を持たせられる。すなわち、二次元配列データからなるデータベースを暗号化する場合などにおいては、データベース検索のキーワードとなる項目が登録されているフィールドに、「このブロックを暗号化しない」という属性を与えておくことにより、キーワードを暗号化しないまま、他のデータを暗号化することが出来る。すると、データベースを検索する場合、データベース全体を復号化しなくても、キーワード検索することができ、検索の結果得られたエントリを必要に応じて復号化して使用することが可能となる。従って、データベース全体を復号化する必要がないので、データベースのある項目のデータを見る権利を得ていないユーザには、その項目のデータを隠したまま、そのユーザにデータベースの使用をさせるということが可能となる。

【００１７】

また、データベースでなくても、例えば、画像データを本発明の実施形態に従って、暗号化した場合、企業秘密など、特定のユーザにしか見せたくない部分は、他の部分の暗号鍵と異なる暗号鍵を使って暗号化しておくことにより、その部分のみは秘密にしたまま当該画像データの使用を他のユーザに許可することが可能となる。

【００１８】

図３は、属性データの格納方法の例を概念的に示す図である。

第１の実施形態では、暗号の二次元配列データ｛Ｃｎ｝と属性のデータ｛Ａｎ｝とを別々に管理することを考えている。すなわち、暗号化データ｛Ｃｎ｝と属性データ｛Ａｎ｝は、別ファイルとして記録媒体に記録され、復号化の際、属性データ｛Ａｎ｝を、対応する暗号化データ｛Ｃｎ｝に適用して復号化することにより、元の平文Ｍを得るようにする。しかし、例えば、図３（ａ）、（ｂ）に示

すように｛Ａｎ｝と｛Ｃｎ｝を一つのデータとしてまとめて管理する様にしても良い。すなわち、図３（ａ）と図３（ｂ）は、暗号化データ｛Ｃｎ｝と属性｛Ａｎ｝とを互いの対応関係が分かるようにした上で、一つのファイルとして格納するものである。図３（ａ）では、暗号データ｛Ｃｎ｝の格納領域の一部に属性｛Ａｎ｝を格納し、復号する際には、まず、復号するデータ領域を取得し、これから、属性｛Ａｎ｝を先に読み出し、次に、暗号化データ｛Ｃｎ｝を読み出すことによって、復号化処理を行うようにする。あるいは、図３（ｂ）に示されてるように、暗号化データ群｛Ｃｎ｝の先頭に属性データ群｛Ａｎ｝を付加するようにして、記録媒体に格納しても良い。復号化する際には、最初に属性データ群｛Ａｎ｝を読み込み、次に、読み込んだ属性データＡｎに対応する暗号化データＣｎを読み込んで復号化するようにする。特に、図３（ｂ）の場合には、属性データ群｛Ａｎ｝のそれぞれにどの暗号化データＣｎに対応する属性データであるかを示す識別子などを付加しておく。

【００１９】

また、上記第１の実施形態では、平文の二次元配列データを任意の形状のブロックに分け、各ブロックに付与して定義した暗号化の属性によって当該ブロックを暗号化したが、その変形例としては、平文の二次元配列データをブロックに分け、それに暗号化の属性を規定した上で、そのブロックを更に微小な領域（サブブロック）に分け、その各々のサブブロックの暗号化に新たな属性を設定し、サブブロック毎に暗号化する方法が可能である。

【００２０】

上記変形例では、第１の実施形態での平文の二次元配列データを分割して得られるブロックを、更に微小なサブブロックに分割して、その各サブブロックに新たな暗号化の属性を設定している。このため、属性の階層化が実現され、これを基にセキュリティ管理の階層化がなされるという効果がある。すなわち、人事管理のデータベースの暗号化にこの変形例を適用した場合には、人事部の平社員には、社員の名前と住所、電話番号を検索することが出来るが、給与所得や社員のプライベートに関する情報は、人事部の幹部社員にしかみれないように、暗号鍵を設定することが出来る。

【００２１】

この変形例では、平文をブロック化して、その各々のブロックに暗号化の属性を設定した後、各ブロックを更にサブブロックに分け、こうして得られたサブブロックに新たな暗号化の属性を設定したが、この前者の手続によって得られた「ブロックを」サブブロックと見なし、その幾つかのブロックをひとまとめにして得られる巨大ブロック（クラスタ）を構成し、各クラスタに新たな暗号化の属性を持たせることも可能である。この場合、平文のブロックに関する階層構造は、上記変形例のものと形式的には同じ構造になるが、暗号化の属性の階層構造は、逆転する。

【００２２】

また、更なる変形例では、上記変形例のように「ブロック」をサブブロックに分割し、そのサブブロック毎に暗号化を行うのではなく、ブロックを暗号化した後、サブブロックに分割し、そのサブブロックを暗号化しても良い。

【００２３】

図４は、属性データを格納する属性テーブルの構成例を示した図である。

属性テーブルは、平文のブロック毎に、１レコードずつが設けられる。そして、１レコードには、平文である画像データをブロックに区分けしたときのブロックの起点アドレス（「ビット矩形起点」、この場合、ブロックは矩形としている）、「ビット矩形サイズ」（ピクセル単位のブロックの大きさをビットで表したもの）、アクセス特権（どのようなユーザが復号化してアクセスする権利を有するかを規定する値）、鍵長、暗号鍵が格納される。図３（ａ）のように属性テーブルを格納する場合には、各レコードはバラバラに各暗号化ブロックに添付される。また、これらは、全ての平文のブロックについて異なっていても良いし、複数のブロックについては同じ情報が格納されていることもあり得る。

【００２４】

図５は、暗号化プロセスを示すフローチャートである。

まず、ステップＳ１０において、暗号化属性を確認しながら属性テーブルを作成する。この属性の入力は、例えば、平文データを暗号化するユーザが入力する。そして、ステップＳ１１において、平文を読み込む。ステップＳ１２において

、属性テーブルに基づいて平文を暗号化し、ステップＳ１３において、暗号を書き出し、同時に属性も書き出す。これにより、暗号化データと、属性テーブルが生成される。暗号化データと属性テーブルの保存の仕方は、前述したように、別ファイルとして、格納しても良いし、暗号化データと属性テーブルを組み合わせて、１つのファイルとして格納しても良い。そして、ステップＳ１４において、ユーザに暗号化処理を終了するか否かの入力を求め、終了しない場合には、ステップＳ１１に戻って、処理を繰り返し、終了する場合には、そのまま処理を終了する。

【００２５】

図６は、復号化プロセスを示すフローチャートである。

まず、ステップＳ２０において、暗号データの読み込みと、属性テーブルからの属性の読み込みを行う。そして、ステップＳ２１において、属性テーブルに基づいて暗号を復号化し、ステップＳ２２において、復号された平文データを書き出す。そして、ステップＳ２３において、ユーザに復号化処理を終了するか否かの指示を求め、終了しない場合には、ステップＳ２０に進み、終了する場合には、そのまま処理を終了する。

【００２６】

図７～図１０は、サブブロック分割を行った場合の暗号化処理を示すフローチャートである。

図７においては、まず、ステップＳ３０において、平文データである二次元配列データを分割して、ブロック化する。そして、ステップＳ３１において、各ブロックへ、暗号化属性の設定を行う。この設定は、例えば、ユーザが行う。そして、ステップＳ３２において、各ブロックへの分割した後に、更に、各ブロックをサブブロックに分割する。そして、ステップＳ３３において、各サブブロックへ暗号化属性を設定する。この設定も、例えば、ユーザが行う。そして、ステップＳ３４において、各サブブロックを暗号化して処理を終了する。なお、この場合、サブブロックの暗号化のみ行っているが、サブブロックの暗号化の際に、サブブロックに設定された属性のみではなく、元のブロックに設定された属性も反映させるようにすることが望ましい。例えば、アクセス特権の設定について述べ

れば、サブブロックへのアクセス権は、サブブロックに設定された属性に設定されたアクセス特権のみではなく、元のブロックに設定されたアクセス特権をも満足するユーザにのみ当該サブブロックへのアクセスを許可するようにする。

【００２７】

図８においては、サブブロックと元のブロックの両方を暗号化する。すなわち、ステップＳ４０において、平文データである二次元配列データの分割を行い、平文データのブロック化を行う。そして、ステップＳ４１において、各ブロックへの暗号化属性の設定を、例えば、ユーザが行う。次に、ステップＳ４２において、各ブロックへの分割によるサブブロックを生成し、ステップＳ４３において、各サブブロックへの暗号化属性の設定を、例えば、ユーザが行う。そして、ステップＳ４４において、各サブブロックをサブブロックの暗号化属性に従って、暗号化し、次に、ステップＳ４５において、元の各ブロックに対し、暗号化属性に基づいて暗号化を行う。

【００２８】

図９においては、ブロック化後、各ブロックを暗号化し、その後サブブロック化して、各サブブロックを暗号化する処理である。まず、ステップＳ５０において、平文データである二次元配列データを分割して、ブロック化を行う。そして、ステップＳ５１において、各ブロックへの暗号化属性を、例えば、ユーザが設定し、ステップＳ５２において、各ブロックを暗号化する。次に、ステップＳ５３において、平文データの各ブロックをサブブロックに分割し、ステップＳ５４において、例えば、ユーザが各サブブロックの暗号化属性を設定する。そして、ステップＳ５５において、各サブブロックを暗号化して、処理を終了する。

【００２９】

図１０は、サブブロックを更に小さなブロックに分割していき、順次暗号化するための処理を示す。まず、ステップＳ６０において、平文データである二次元配列データを分割して、ブロック化する。次に、ステップＳ６１において、各ブロックの暗号化属性を、例えば、ユーザが設定する。そして、そして、ステップＳ６２において、各ブロックへの分割によるサブブロックの生成を行い、ステップＳ６３において、各サブブロックの暗号化属性の設定を、例えば、ユーザが行

い、ステップＳ６４において、各サブブロックを暗号化する。そして、ステップＳ６５において、サブブロックを更に小さいブロックに分割して暗号化を行うか否かをユーザに入力させ、ユーザの指示を判断する。処理を継続する場合には、ステップＳ６２に戻り、サブブロックを元のブロックと見なしてサブブロック化とその暗号化を行う。ステップＳ６５において、処理を継続しないと判断された場合には、ステップＳ６６において、１番最初の元ブロックの暗号化を行って、処理を終了する。

【００３０】

なお、上記フローチャートの説明では、ブロック化、サブブロック化の仕方をどのようにするかについては、特に述べなかったが、これは、ユーザに指定によって行っても良いし、特定のアルゴリズムを使って行っても良い。特定のアルゴリズムとしては、二次元配列データを上下左右に２分割ずつする処理を順次繰り返し行うと言うものでも良い。

【００３１】

図１１は、本発明の第２の実施形態の概念を説明する図である。

第１の実施形態においては、データの論理的構造（二次元配列など）に基づいてブロック化することを主眼においたが、本実施形態においては、物理的データの構成をブロック化して暗号化する。

【００３２】

図１１（ａ）は、平文（Ｍ）のストリームデータを模式的に示したものである。このように、記録媒体上では、データは、ストリームデータとして１時限的に配列されている。図１１（ｂ）は、平文を幾つかのブロックに分けたものである。ここに、各ブロックの長さは任意に設定してよく、同一の長さであっても、各々が互いに異なる長さであっても良い。ＭｎとＭに付した番号ｎはブロックの番号を意味する。図１１（ｃ）は、平文のブロックＭｎの暗号化を規定する属性Ａｎのデータ配列を示す。ここでは、ＭｎとＡｎの一対一対応が明確になるように図示されているが、実際には、この対応付けが正確になされれば良く、例えば、ＭｎとＡｎの配列順序が異なっていても、ポインタなどによって一対一に対応付けられていればよい。図１１（ｄ）は、平文のブロックＭｎを暗号化の属性Ａｎ

で暗号化して得られた暗号のブロックＣｎを示している。このように、平文ストリームデータをブロックＭｎに分割し、これを、ブロックＭｎ毎に設けられる属性Ａｎに基づいて暗号化して、暗号化データストリーム｛Ｃｎ｝を得る。

【００３３】

図１１（ａ）～（ｄ）では、平文のブロックＭｎと暗号のブロックＣｎとは同じ長さで表されているが、一般にはこれらの長さは異なっても良い。

暗号のストリームデータ｛Ｃｎ｝と属性｛Ａｎ｝が保存されるため、平文のストリームデータ｛Ｍｎ｝を得るには保存されている暗号のストリームデータ｛Ｃｎ｝に対し｛Ａｎ｝で規定される暗号の属性を基に復号化の操作を行えばよい。

【００３４】

なお、図１１（ａ）～（ｄ）では、平文のストリームデータを幾つかのブロックに分け、その各ブロックの暗号化に属性を設けて暗号化したことにより、第１の実施形態と同様に、ブロック毎の暗号化時に暗号の属性をきめ細かく設定できるという効果がある。例えば「このブロックは暗号化しない」という属性も付与することができ、暗号化データの安全性を損なうことなく、暗号化データを全文検索の対象にし得るという実用上便利な性格を持たせられる。

【００３５】

また、暗号ストリームデータ｛Ｃｎ｝と属性のデータ｛Ａｎ｝とを別々に管理することも可能であるが、図１１（ｅ）と図１１（ｆ）に示すように｛Ａｎ｝と｛Ｃｎ｝とを一つのデータとしてまとめて管理するようにしても良い。図１１（ｅ）の場合には、暗号化された各ブロック｛Ｃｎ｝の先頭に暗号化に使用された属性｛Ａｎ｝が付加されている。この場合、暗号化ブロック｛Ｃｎ｝と属性｛Ａｎ｝が物理的に対応させられているので、先頭から順次、属性｛Ａｎ｝、暗号化ブロック｛Ｃｎ｝と読み込み、属性Ａｎに従って、後続の暗号化ブロックＣｎを復号化することにより平文Ｍｎを得ることが出来る。また、図１１（ｆ）に示すように、暗号ブロック｛Ｃｎ｝の配列の先頭に属性｛Ａｎ｝の配列を配置することも可能である。この場合には、属性｛Ａｎ｝が何番目に配置されているかなどの情報から、対応する暗号化ブロック｛Ｃｎ｝を特定できるようにしておく必要がある。もちろん、属性｛Ａｎ｝に対応する暗号化ブロック｛Ｃｎ｝のアドレス

などを示すポインタを含ませるようにしても良い。

【００３６】

なお、上記実施形態では、平文のストリームデータを任意の長さのブロックに分け、各ブロックに付与して定義した暗号化の属性によって当該ブロックを暗号化した。変形例としては、平文のストリームデータをブロックに分け、それに暗号化の属性を規定した上で、そのブロックを更に微小な領域（サブブロック）に分け、その各々のサブブロックの暗号化に新たな属性を設定し、サブブロック毎に暗号化することも可能である。また、上記変形例では、平文のストリームデータを分割して得られるブロックを、更に微小なサブブロックに分割して、その各サブブロックに新たな暗号化の属性を設定している。このため、属性の階層化が実現され、これを基にセキュリティ管理の階層化がなされるという効果がある。

【００３７】

また、上記変形例では、平文をブロック化して、その各々のブロックに暗号化の属性を設定した後、各ブロックを更にサブブロックに分け、こうして得られたサブブロックに新たな暗号化の属性を設定したが、この前者の手続によって得られた「ブロックを」サブブロックと見なし、その幾つかのブロックをひとまとめにして得られる巨大ブロック（クラスタ）を構成し、各クラスタに新たな暗号化の属性を持たせることも可能である。この場合、平文のブロックに関する階層構造は第２の実施例のものと形式的には同じ構造になるが、暗号化の属性の階層構造は逆転する。

【００３８】

更なる変形例としては、「ブロック」をサブブロックに分割し、そのサブブロック毎に暗号化を行うが、ブロックを暗号化した後、サブブロックに分割し、そのサブブロックを暗号化しても良い。

【００３９】

図１２は、第２の実施形態における属性テーブルの例を示した図である。

平文のストリームデータをブロック化した場合の各ブロックに対し、１レコードが対応する。各レコードには、ブロックの開始位置がビット単位で示される。また、各レコードには、対応する平文ストリームデータのブロックのビット長が

「暗号化ビット長」として、格納されると共に、第１の実施形態と同様に、「アクセス特権」、「鍵長」、「暗号鍵」が登録される。図１１（ｅ）のように属性テーブルを格納する場合には、各レコードがバラバラに、それぞれの暗号化ブロックに添付される。また、これらは、全ての平文のブロックについて異なっていても良いし、複数のブロックについては同じ情報が格納されていることもあり得る。

【００４０】

図１３は、第２の実施形態における暗号化プロセスを示すフローチャートである。

まず、ステップＳ７０において、暗号化属性を確認しながら、属性テーブルを作成する。この暗号化属性は、例えば、ユーザからの入力による。そして、ステップＳ７１において、平文を読み込み、ステップＳ７２において、属性テーブルに基づいて平文を暗号化する。そして、ステップＳ７３において、暗号データと属性データを書き出して、ステップＳ７４において、処理を終了するか否を判断する。ステップＳ７４において、ユーザから処理を続ける旨の指示があった場合には、ステップＳ７１に戻って、処理を継続する。ステップＳ７４において、ユーザから処理を終了する旨の指示があった場合には、処理を終了する。

【００４１】

なお、暗号データと属性データの格納の仕方は、前述したとおり、様々な方法が可能である。

図１４は、第２の実施形態における復号化プロセスを示すフローチャートである。

【００４２】

まず、ステップＳ８０において、暗号データ（暗号文）と属性を読み込む。そして、ステップＳ８１において、属性テーブルに基づいて暗号データを復号化し、ステップＳ８２において、平文を書き出す。そして、ステップＳ８３において、ユーザに処理を終了するか否かを尋ね、終了しない場合には、ステップＳ８０に進み、商量する場合には、そのまま処理を終了する。

【００４３】

図１５～図１８は、第２の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャートである。

図１５においては、まず、ステップＳ９０において、平文ストリームデータを分割し、ブロック化する。そして、ステップＳ９１において、各ブロックの暗号化属性をユーザに設定させる。そして、ステップＳ９２において、各ブロックの分割によるサブブロックの生成を行い、ステップＳ９３において、各サブブロックの暗号化の属性をユーザに設定させ、ステップＳ９４において、各サブブロックを暗号化して処理を終了する。なお、この場合、サブブロックの暗号化のみ行っているが、サブブロックの暗号化の際に、サブブロックに設定された属性のみではなく、元のブロックに設定された属性も反映させるようにすることが望ましい。例えば、アクセス特権の設定について述べれば、サブブロックへのアクセス権は、サブブロックに設定された属性に設定されたアクセス特権のみではなく、元のブロックに設定されたアクセス特権をも満足するユーザにのみ当該サブブロックへのアクセスを許可するようにする。

【００４４】

図１６においては、まず、ステップＳ１００において、平文ストリームデータを分割し、ブロック化する。そして、ステップＳ１０１において、各ブロックの暗号化属性をユーザに設定させる。そして、ステップＳ１０２において、各ブロックを分割して、サブブロックを生成する。そして、ステップＳ１０３において、各サブブロックの暗号化属性をユーザに設定させ、ステップＳ１０４において、各サブブロックの暗号化を行い、ステップＳ１０５において、各元ブロックの暗号化を行って処理を終了する。

【００４５】

図１７においては、ステップＳ１１０において、平文ストリームデータの分割を行い、ブロック化を行う。そして、ステップＳ１１１において、各ブロックの暗号化属性をユーザに設定させ、ステップＳ１１２において、各ブロックを暗号化する。そして、ステップＳ１１３において、暗号化後の各ブロックを分割し、サブブロックを生成する。そして、ステップＳ１１４において、各サブブロックの暗号化属性をユーザに設定させ、ステップＳ１１５において、各サブブロック

の暗号化を行い、処理を終了する。

【００４６】

図１８においては、ステップＳ１２０において、平文ストリームデータの分割を行い、ブロック化を行う。そして、ステップＳ１２１において、各ブロックの暗号化属性をユーザに設定させる。そして、ステップＳ１２２において、各ブロックの分割によるサブブロックの生成を行い、ステップＳ１２３において、各サブブロックの暗号化属性をユーザに設定させ、ステップＳ１２４において、各サブブロックを暗号化し、ステップＳ１２５において、ユーザから処理を継続するか否かの指示を判断する。処理を継続する場合には、ステップＳ１２２に戻って、サブブロックを元ブロックと見なして処理を繰り返し行う。ステップＳ１２５において、処理を継続しない旨判断された場合には、ステップＳ１２６に進んで、元ブロックの暗号化を行い、処理を終了する。

【００４７】

図１９は、暗号化装置のブロック構成図である。

暗号化装置１０においては、まず、平文入力部１１に平文データが入力される。また、平文入力部１１には、ブロック化部１５が設けられており、平文データをブロック化する。そして、ブロック化された平文データは、属性設定部１２に入力され、各ブロック毎にユーザから属性が設定される。そして、ブロック化された平文データは、暗号化部１３に入力され、当該ブロックに設定された属性に基づいて暗号化される。サブブロック化する場合には、平文データが平文入力部１１に入力された時点で、サブブロックまでブロック化するか、あるいは、暗号化部１３でブロック単位で暗号化された後、暗号化文を平文入力部１１に入力して、ブロック化部１５を用いて、サブブロック化し、属性設定部１２において、サブブロックに属性を設定する。このようにして、暗号化された平文データは、暗号文データとして、暗号文、属性テーブル出力部１４に送られる。また、属性設定部１２からは、属性テーブルが暗号文、属性テーブル出力部１４に送られ、暗号文データと属性テーブルが出力される。

【００４８】

図２０は、復号化装置のブロック図である。

復号化装置２０においては、暗号文データと属性テーブルが暗号文、属性テーブル入力部２１に入力される。これは、復号化部２２に入力され、属性テーブルを参照しながら、暗号文データが復号化され、平文データが復元される。そして、平文データは、平文出力部２３から平文が出力される。

【００４９】

図２１は、本発明の実施形態の処理をプログラムで実現する場合に必要とされる情報装置のハードウェア環境を示す図である。

情報装置４１は、バス３０に、ＣＰＵ３１、ＲＯＭ３２、ＲＡＭ３３、通信インターフェース３４、記録装置３７、記録媒体読み取り装置３８、入出力装置４０が接続されて構成される。ＲＯＭ３２には、ＢＩＯＳなどの基本プログラムが格納され、情報装置４１の起動時にＣＰＵ３１がＲＯＭ３２から読み込むことによって、入出力装置４０や記録装置３７などを利用可能とする。本発明の実施形態を実現する当該プログラムは、ハードディスクなどの記録装置３７や、ＣＤ－ＲＯＭ、ＤＶＤ、ＭＯ、フロッピーディスクなどの可搬記録媒体３９に格納され、記録装置３７から直接ＲＡＭ３３に読み込むか、記録媒体読み取り装置３８を介して、可搬記録媒体３９からＲＡＭ３３に読み込まれ、ＣＰＵ３１が実行可能な状態とされる。また、平文は、キーボード、マウス、ディスプレイ、スキャナなどからなる入出力装置４０からＲＡＭ３３に読み込まれたり、可搬記録媒体３９や記録装置３７からＲＡＭ３３に読み込まれることによって、ＣＰＵ３１が暗号化可能とする。暗号文は、可搬記録媒体３９や記録装置３７に格納される。また、同時に、暗号化処理において生成される属性テーブルも可搬記録媒体３９や記録装置３７に格納される。

【００５０】

また、情報装置４１は、通信インターフェース３４を用いて、ネットワーク３５に接続し、情報提供者３６から当該プログラムをダウンロードして実行することも可能である。また、平文を情報装置４１側で暗号化し、暗号文と属性テーブルとをネットワーク３５を介して情報提供者３６に送信することによって、暗号文による通信をすることができる。また、情報提供者３６が有する平文をネットワーク３５を介して受信し、情報装置４１で暗号化して、情報提供者３６に送信

すれば、情報提供者３６に代わって、暗号化処理を代行することも可能である。また、復号についても代行が可能である。更に、当該プログラムは、ネットワーク３５を介して、情報提供者３６と情報装置４１が接続された状態で、すなわち、ネットワーク環境の下に実行することも可能である。

【００５１】

【発明の効果】

本発明によれば、１つの平文データを暗号化する場合にも、平文データの部分部分で暗号化の仕方などを変えることができるので、暗号文の一部が解読されても、他の部分が解読されず、より暗号の信頼性を高めることが出来る。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態の概念を説明する図（その１）である。

【図２】

本発明の第１の実施形態の概念を説明する図（その２）である。

【図３】

属性データの格納方法の例を概念的に示す図である。

【図４】

属性データを格納する属性テーブルの構成例を示した図である。

【図５】

暗号化プロセスを示すフローチャートである。

【図６】

復号化プロセスを示すフローチャートである。

【図７】

サブブロック分割を行った場合の暗号化処理を示すフローチャート（その１）である。

【図８】

サブブロック分割を行った場合の暗号化処理を示すフローチャート（その２）である。

【図９】

サブブロック分割を行った場合の暗号化処理を示すフローチャート（その３）である。

【図１０】

サブブロック分割を行った場合の暗号化処理を示すフローチャート（その４）である。

【図１１】

本発明の第２の実施形態の概念を説明する図である。

【図１２】

第２の実施形態における属性テーブルの例を示した図である。

【図１３】

第２の実施形態における暗号化プロセスを示すフローチャートである。

【図１４】

第２の実施形態における復号化プロセスを示すフローチャートである。

【図１５】

第２の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート（その１）である。

【図１６】

第２の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート（その２）である。

【図１７】

第２の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート（その３）である。

【図１８】

第２の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート（その４）である。

【図１９】

暗号化装置のブロック構成図である。

【図２０】

復号化装置のブロック図である。

【図２１】

本発明の実施形態の処理をプログラムで実現する場合に必要とされる情報装置のハードウェア環境を示す図である。

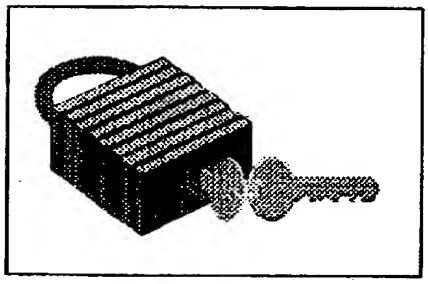
【符号の説明】

１０	暗号化装置
１１	平文入力部
１２	属性設定部
１３	暗号化部
１４	暗号文、属性テーブル出力部
１５	ブロック化部
２０	復号化部
２１	暗号文、属性テーブル入力部
２２	復号部
２３	平文出力部

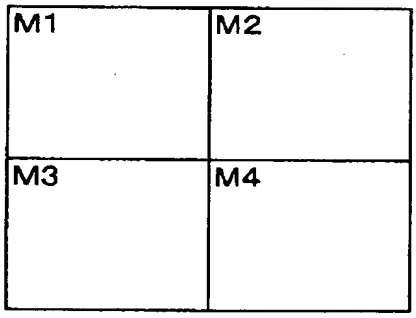
【書類名】　　図面

【図１】

本発明の第1の実施形態の概念を説明する図(その1)



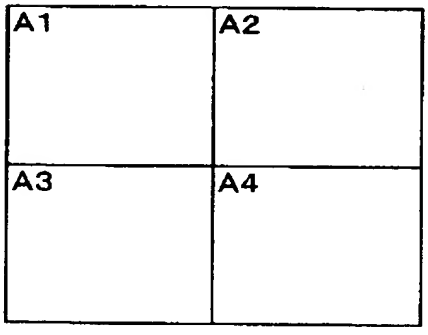
(a)



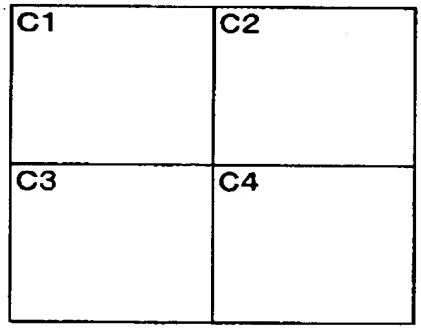
(b)

【図２】

本発明の第1の実施形態の概念を説明する図(その2)



(a)

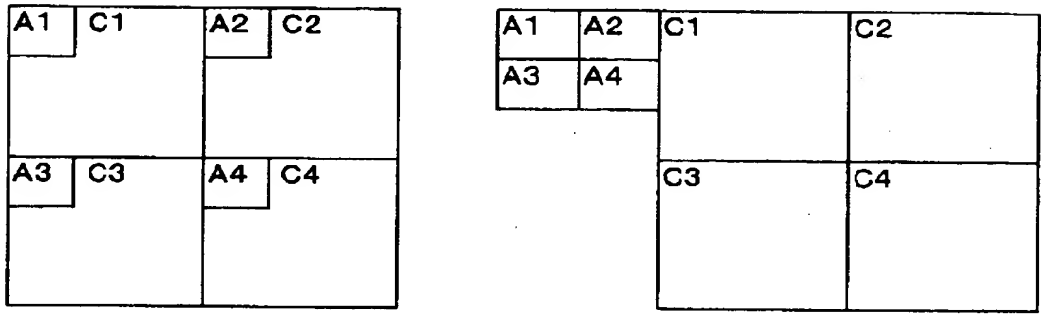


(b)

出証特２００１－３０１７２６８

【図３】

属性データの格納方法の例を概念的に示す図



(a)　　(b)

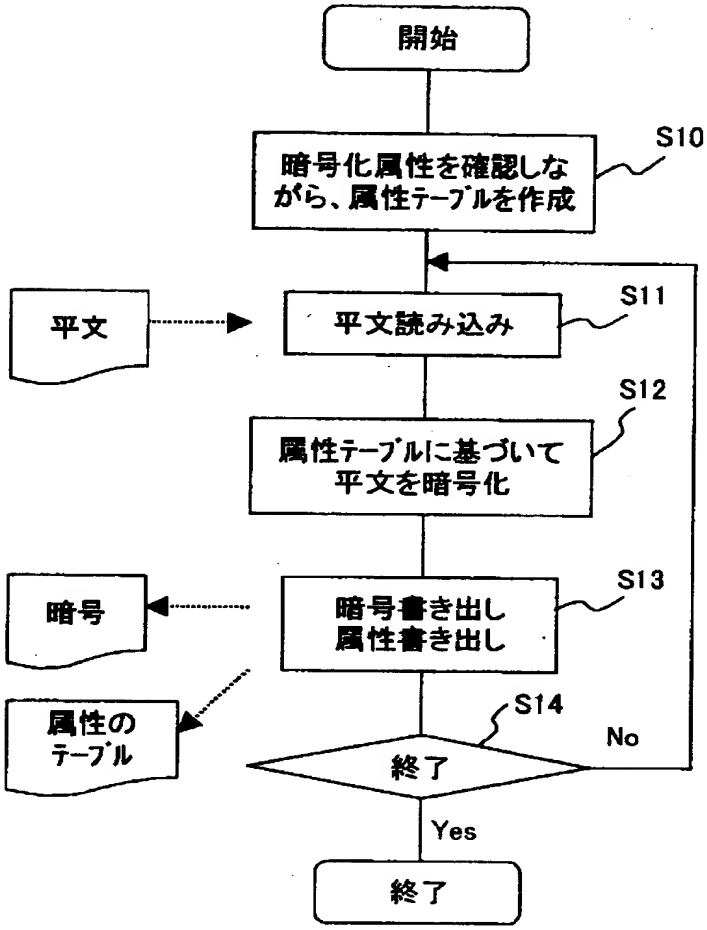
【図４】

属性データを格納する属性テーブルの構成例を示した図

ﾚｺｰﾄﾞ1	ﾋﾞｯﾄ矩形起点	ﾋﾞｯﾄ矩形ｻｲｽﾞ	ｱｸｾｽ特権	鍵長	暗号鍵
ﾚｺｰﾄﾞ2	ﾋﾞｯﾄ矩形起点	ﾋﾞｯﾄ矩形ｻｲｽﾞ	ｱｸｾｽ特権	鍵長	暗号鍵
ﾚｺｰﾄﾞ3	ﾋﾞｯﾄ矩形起点	ﾋﾞｯﾄ矩形ｻｲｽﾞ	ｱｸｾｽ特権	鍵長	暗号鍵
ﾚｺｰﾄﾞ4	ﾋﾞｯﾄ矩形起点	ﾋﾞｯﾄ矩形ｻｲｽﾞ	ｱｸｾｽ特権	鍵長	暗号鍵
...					

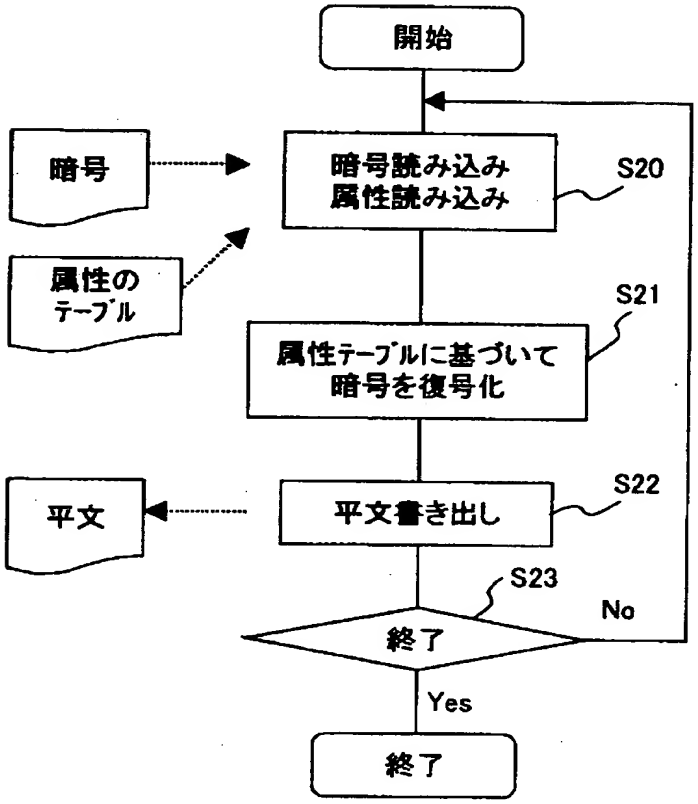
【図５】

暗号化プロセスを示すフローチャート



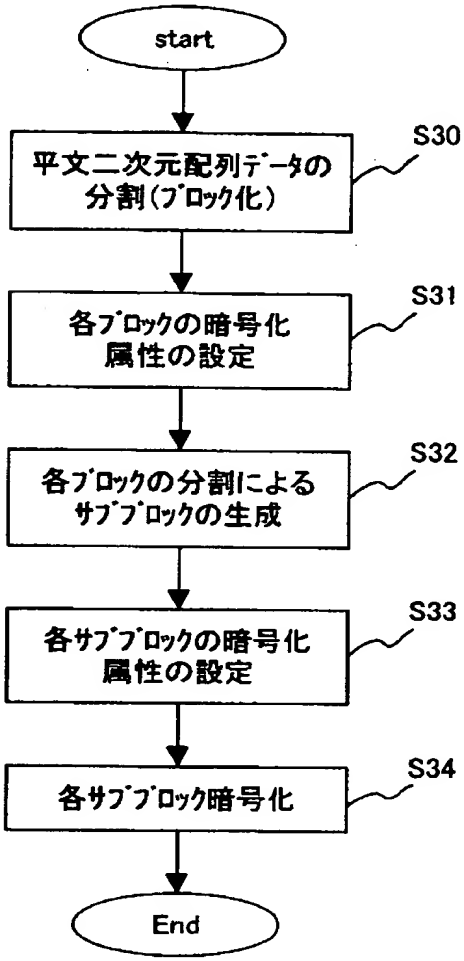
【図６】

復号化プロセスを示すフローチャート



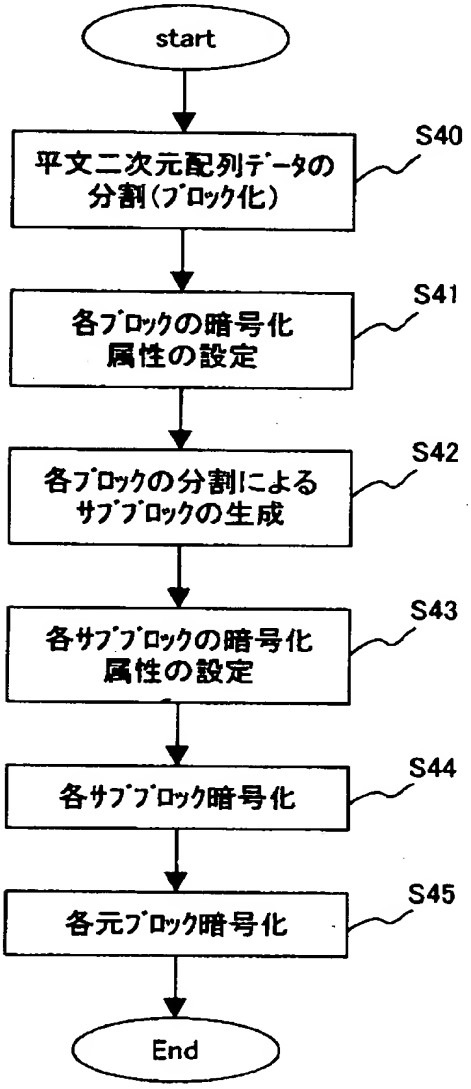
【図７】

サブブロック分割を行った場合の暗号化処理を示すフローチャート（その１）



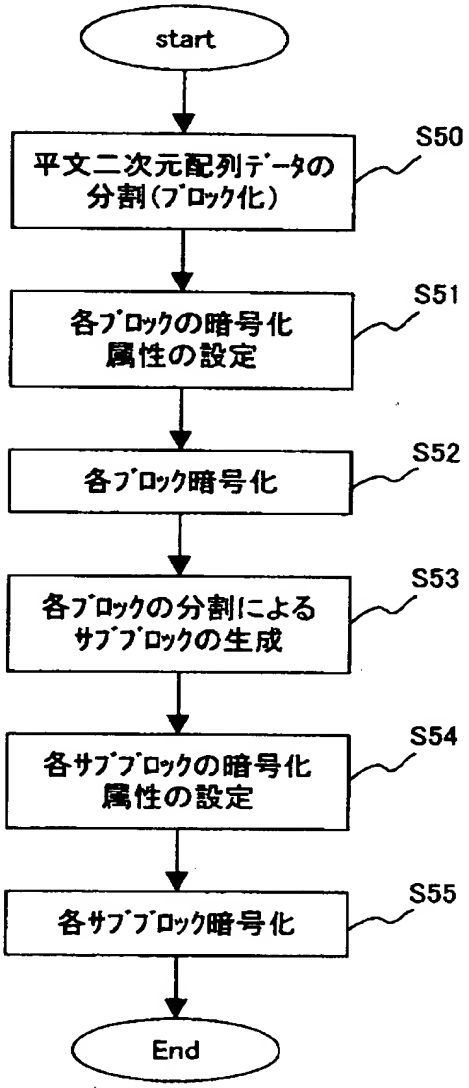
【図８】

サブブロック分割を行った場合の暗号化処理を示すフローチャート(その2)



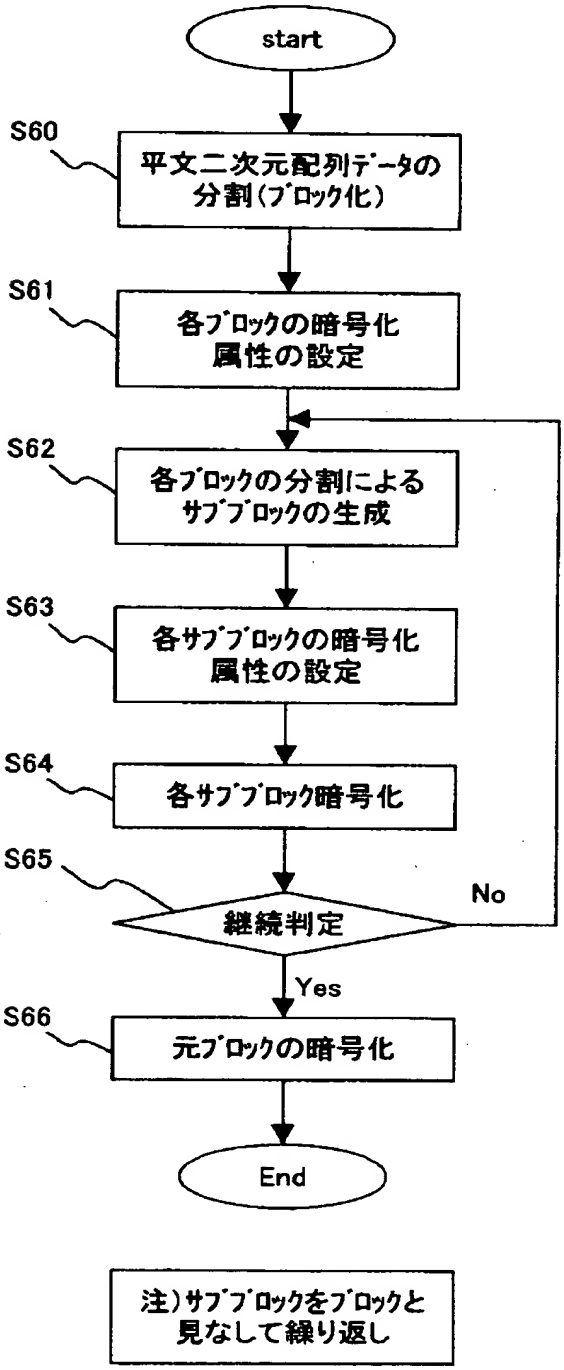
【図９】

サブブロック分割を行った場合の暗号化処理を示すフローチャート(その3)



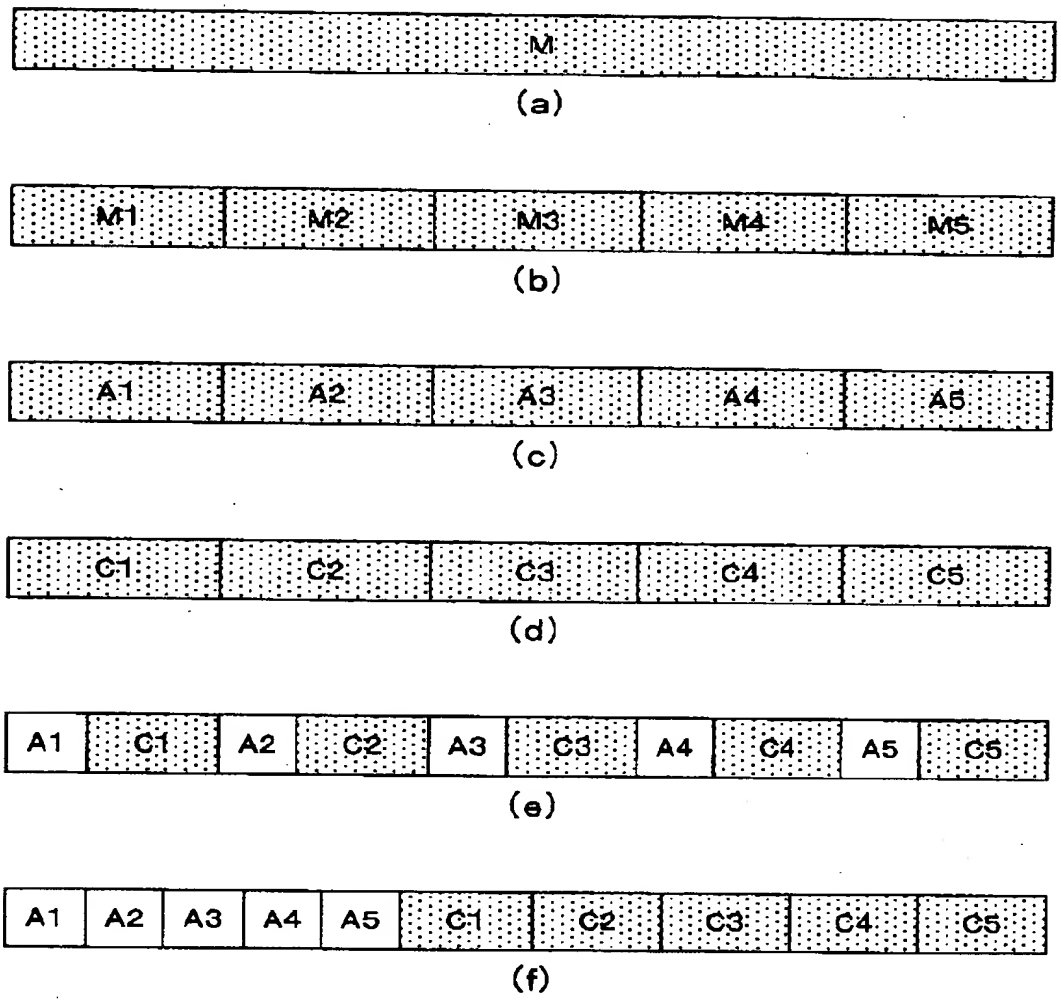
【図１０】

サブブロック分割を行った場合の暗号化処理を示すフローチャート(その4)



【図１１】

本発明の第2の実施形態の概念を説明する図



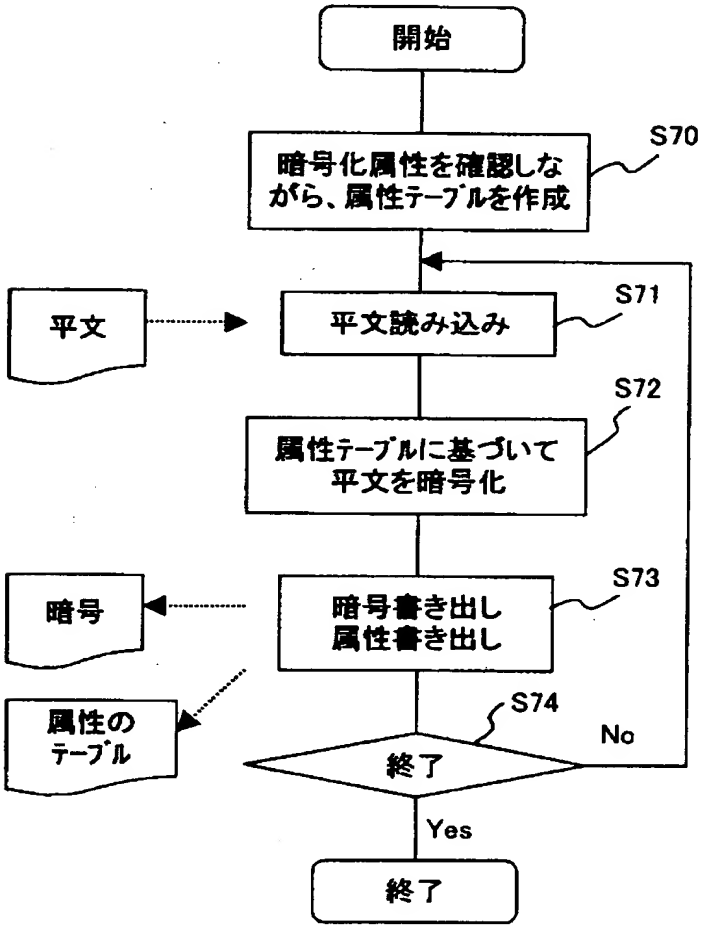
【図１２】

第2の実施形態における属性テーブルの例を示した図

ﾚｺｰﾄﾞ1	ﾋﾞｯﾄ開始位置	暗号化ﾋﾞｯﾄ長	ｱｸｾｽ特権	鍵長	暗号鍵
ﾚｺｰﾄﾞ2	ﾋﾞｯﾄ開始位置	暗号化ﾋﾞｯﾄ長	ｱｸｾｽ特権	鍵長	暗号鍵
ﾚｺｰﾄﾞ3	ﾋﾞｯﾄ開始位置	暗号化ﾋﾞｯﾄ長	ｱｸｾｽ特権	鍵長	暗号鍵
ﾚｺｰﾄﾞ4	ﾋﾞｯﾄ開始位置	暗号化ﾋﾞｯﾄ長	ｱｸｾｽ特権	鍵長	暗号鍵
...					

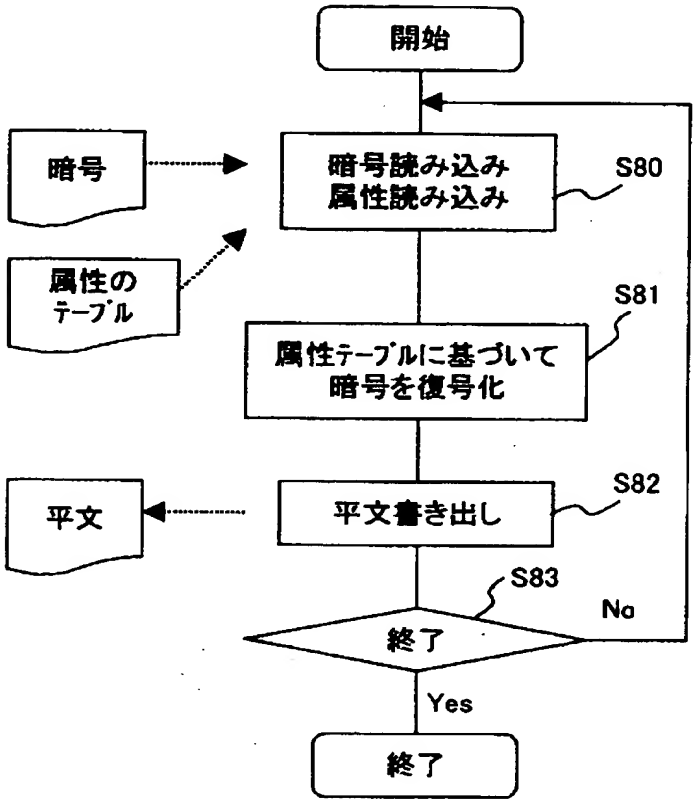
【図１３】

第2の実施形態における暗号化プロセスを示すフローチャート



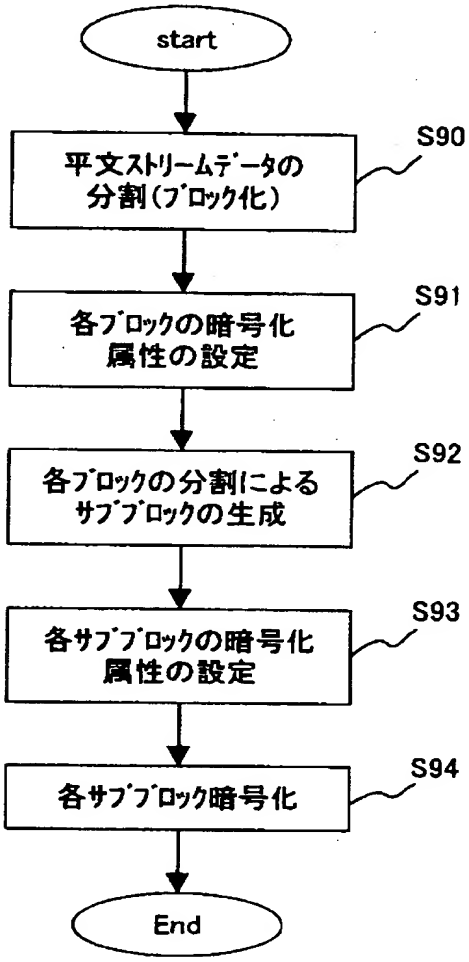
【図１４】

第2の実施形態における復号化プロセスを示すフローチャート



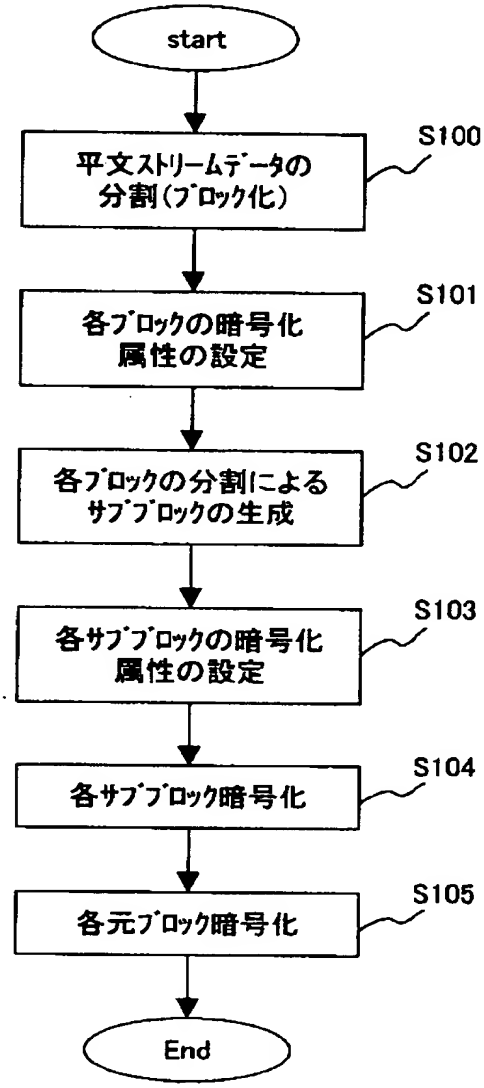
【図１５】

第2の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート(その1)



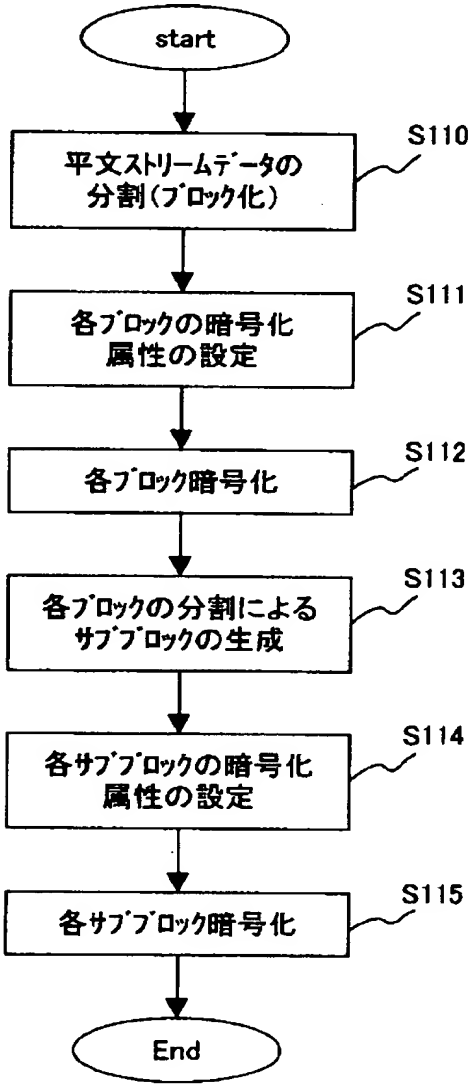
【図１６】

第2の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート(その2)



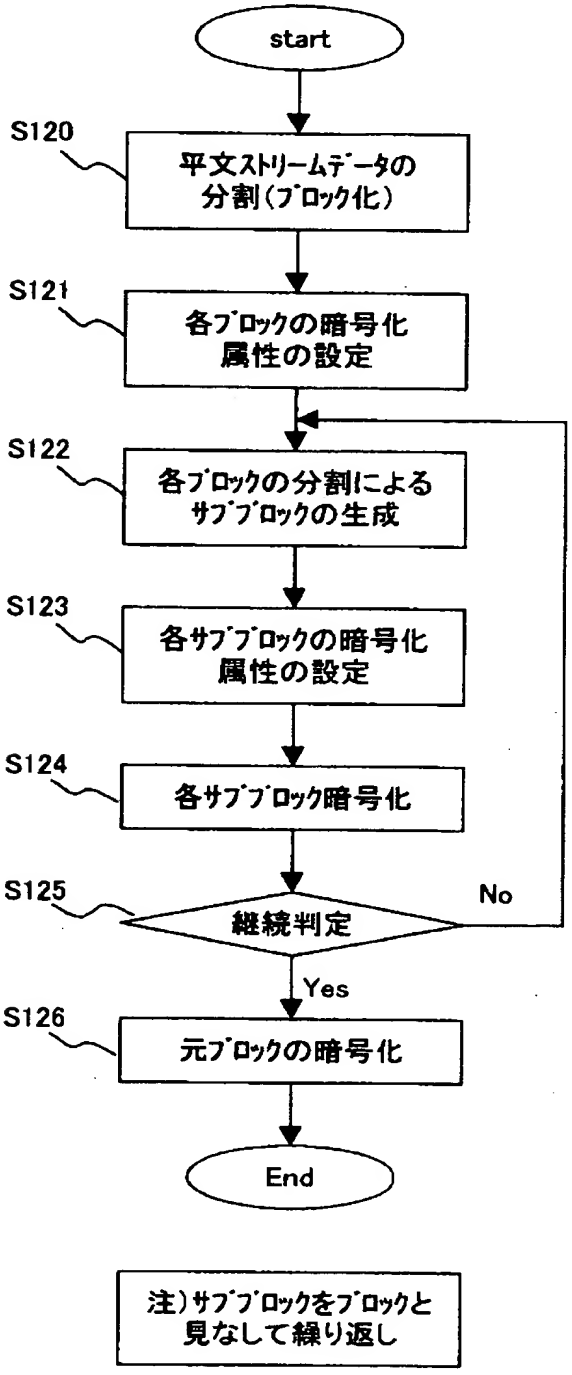
【図１７】

第2の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート(その3)



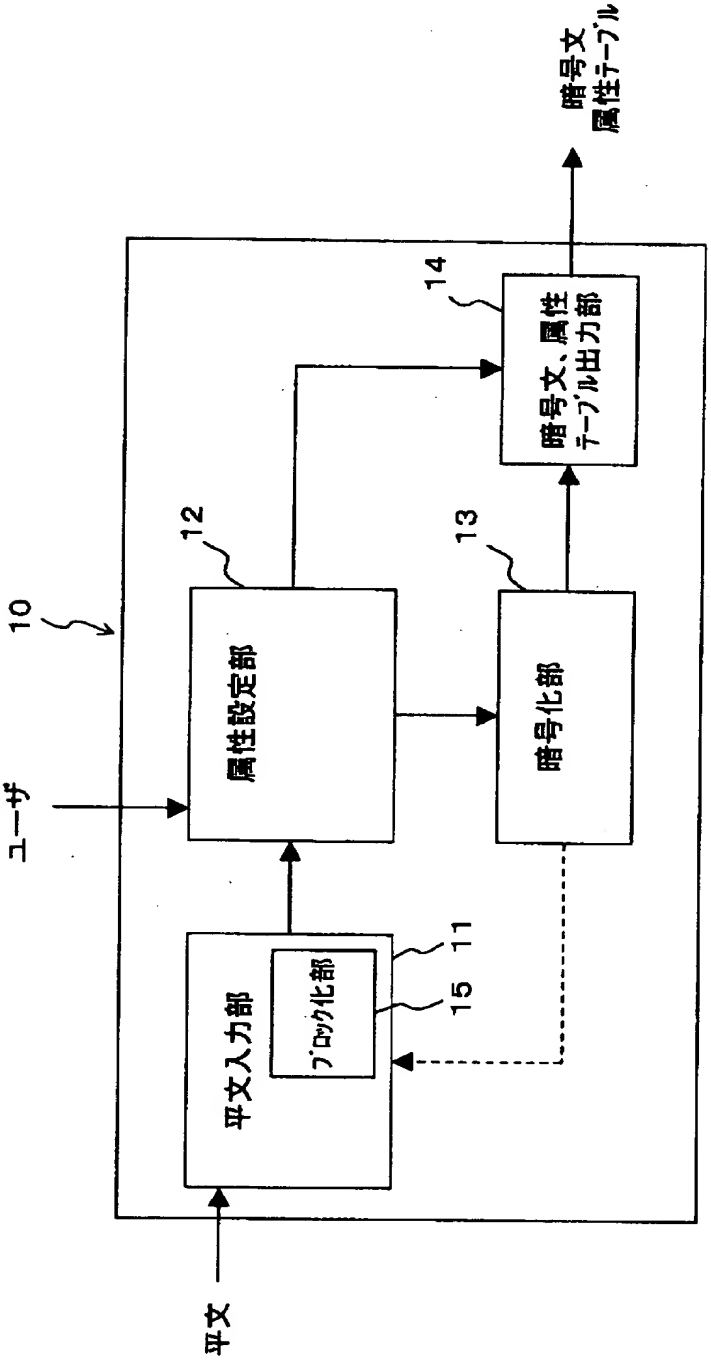
【図１８】

第2の実施形態におけるサブブロックに分割して暗号化する際の暗号化処理を示すフローチャート(その4)



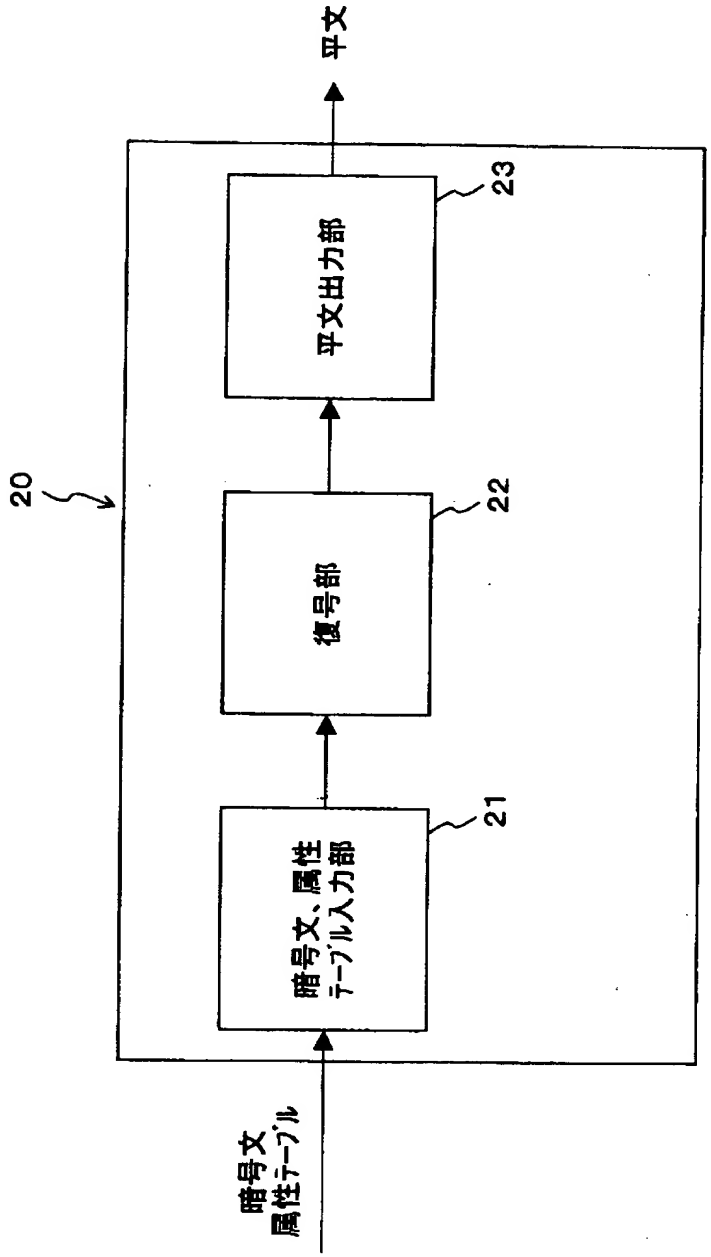
【図１９】

暗号化装置のブロック構成図



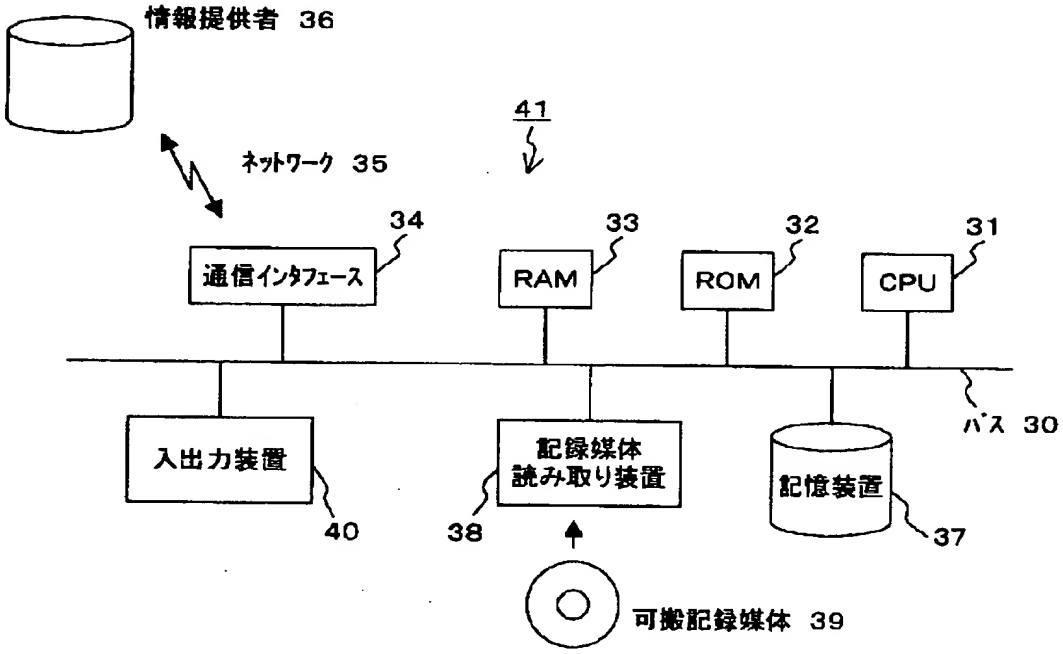
【図２０】

復号化装置のブロック図



【図２１】

本発明の実施形態の処理をプログラムで実現しようとする場合に必要とされる情報装置のハードウェア環境を説明する図



【書類名】　　要約書

【要約】

【課題】データの一部が解読されても全データは容易には解読されない暗号手法を用いた暗号化装置を提供する。

【解決手段】平文データが一次元的あるいは多次元的な構成を論理的あるいは物理的に有している場合、この平文データをブロックに分割し、それぞれに暗号化に際して使用する暗号化属性を設定する。そして、各ブロックをブロック毎に設定された暗号化属性に従って暗号化し、暗号化されたブロックを集めて、暗号文データとする。復号化する場合には、各ブロックに対応した暗号化属性を参照して、各ブロック毎に復号し、復号した結果を集めて、元の平文を得る。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００１４４３〕

１．変更年月日　　１９９８年　１月　９日
［変更理由］　住所変更
住　所　　東京都渋谷区本町１丁目６番２号
氏　名　　カシオ計算機株式会社